Fraud Best Practices Checklist

Banking & Security · https://missionsupport.archden.org/knowledgebase/fraud-best-practices-checklist-2/

Fraudsters continue to evolve their attack strategies.

Business Email Compromise is the most common and successful tactic for tricking AP departments into believing they are legitimate vendors, staff, senior management and more to compromise payment systems. Fraudsters are also following overall payments trends and increasing attacks on payments by ACH and wires as well as through trusted vendors and third-parties. To combat fraud before it happens, companies MUST have well-established work-flows, on-going employee training, and systems in place, especially in today’s environment of remote working and staffing fluctuations. Use the fraud best practices below to assess your company’s potential vulnerabilities.



Download Checklists

Fraud Prevention Best Practices

Employee Training

- Educate on recognizing Business Email Compromise
- Run drills on identifying Phishing attempts

- Adhere to payments work-flows, protocols and systems
- Trust their gut – many fraud attempts have been prevented because something didn't "feel right"

Controls Policy Checklist

- Follow predefined payment instructions; never vary unless changes are thoroughly verified
- Verify legitimacy then validate changes to existing invoices, bank deposit info, and contact info
- Perform call back verification for all funds transfer requests using phone numbers on file for authorized contacts, NOT numbers in an email
- Prohibit initiating payments based on email of other less secure messaging systems
- Require authorized sign-off from senior management for transactions over a certain threshold
- Require multi-factor authentication for access to company network and payments initiation
- Strictly limit the number of employees who have the authority to approve and/or conduct wore transfers or ACH
- Segregation of duties – require different individuals to process collections, disbursements and reconciliation
- Daily reconciliation of accounts
- Do not leave mail unattended
- Shred documents containing sensitive or financial information
- Lock up check stock
- Lock up laptops when not in use

Minimize Checks

- Never approve a wire transfer until appropriate verifications are performed.
- Require dual approval for all wire transfer requests and carefully inspect those with"
    - A dollar amount over a specific threshold
    - Any new trading partners
    - Trading partners not on an approved list to receive wire payments
    - New bank and/or account numbers for current trading partners

- International wire transfers

ACH Controls

- Dual control for ACH file initiation
- Daily reconciliation to identify and return unauthorized ACH debits
- Block all ACH debits except for a single account set up with ACH debit filter or positive pay

Fraud Prevention Best Practices

Check Fraud

- Payee mismatch
- Incorrect amount
- Check number jump
- Duplicate checks
- Monitor check stock

ACH Fraud

- Unauthorized debits
- Payee mismatch
- Incorrect amount
- Inactive account

Business Email Compromise

- Email grammar
- Payee changes
- Urgency

- Contact information change
- Suspicious documents

Insider Fraud

- Prior convictions
- Financial difficulties
- Living beyond means
- Won’t share duties
- Refuses PTO

Ransomware Vulnerabilities

- Outdated software
- Unrestricted user access
- Ineffective firewall
- Automatic download
- Unscanned email

Fraud Management Tools can help protect you.

- ACH Positive Pay
- Alerts
- Check Positive Pay
    - Payee Positive Pay

For more information contact your banker or visit CitywideBanks.com.

Download Checklists